

Re: Web app security

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.aspnet/2008-10/msg01705.html>

- *From:* "SAL" <SAL@xxxxxxxxxxxxxx>
 - *Date:* Wed, 29 Oct 2008 13:13:30 -0700
-

Steven,
thanks for the reply and sorry I'm slow at responding. We've been working on this and trying to get it straight. Our Cold Fusion guy is not able to give me all the details of how his function works so, I found this code example on the internet and we've made some progress. However, it's still a little odd on his end. We started with simple DES encryption as that's the example I found. We are also just using static key and IV's just for testing purposes.

My code:

```
sEncryptionKey = "ABCDEFGH"  
stringToEncrypt = "mystring"  
  
public static string EncryptToBase64String(string stringToEncrypt, string  
SEncryptionKey)  
{  
// http://forums.asp.net/t/222886.aspx  
// Doc for this code  
byte[] key =  
System.Text.Encoding.UTF8.GetBytes(SEncryptionKey.Substring(0, 8));  
byte[] iv = {80,108,67,75,101,121,87,83}; //this is the same as  
in the CF Code = PICKeyWS  
DESCryptoServiceProvider des = new DESCryptoServiceProvider();  
byte[] inputByteArray = Encoding.UTF8.GetBytes(stringToEncrypt);  
MemoryStream ms = new MemoryStream();  
CryptoStream cs = new CryptoStream(ms, des.CreateEncryptor(key,  
iv), CryptoStreamMode.Write);  
cs.Write(inputByteArray, 0, inputByteArray.Length);  
cs.FlushFinalBlock();  
return Convert.ToBase64String(ms.ToArray());  
}  
  
returns: WIViP9S+Q1f5dd+Ox1m3oA==
```

His code:

<cfscript>

Re: Web app security

```

theKey = ToBase64("ABCDEFGH");
Vector = ToBase64("PICKeyWS");
baseVector = ToBinary(Vector);
decrypted = decrypt(URL.P, theKey, "DES/CBC/NoPadding", "BASE64",
baseVector);
parameters = ListToArray(decrypted, "&");
</cfscript>

<cfdump var="#parameters#">

```

But, his output is:
mystring

We don't understand the boxes on his output. However, if he encrypts, his results are only the same as mine if he includes the boxes. We are wondering if we could get any insight into why this is happening. Once we get it straight, we'd also like to move on to better encryption such as AES.

Thanks
S

""Steven Cheng"" <stcheng@xxxxxxxxxxxxxxxxxxxxxx> wrote in message news:k4cdbzKOJHA.356@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi SAL,

From your description, I understand that you're encountering some problem to make the.NET AES encryption to work together with the AES encryption component in Adobe codefusion system, correct?

Based on the codesnippet and encrypt info you provided, I think here are something we need to clarify first:

#AES support various key length and may have customized chain mode, you can print the default settings (when you create the RijndaelManaged provider) and confirm the setting with your CodeFusion side guys:

```

=====
RijndaelManaged AESP = new RijndaelManaged();
string str = string.Format("feedback mode:{0},key
size:{1},Padding:{2}", AESP.Mode.ToString(), AESP.KeySize, AESP.Padding);
MessageBox.Show(str);
=====

```

here is the output from my side:

```

-----
feedback mode:CBC,key size:256,Padding:PKCS7

```

Re: Web app security

In addition, when you use .NET AES(Rnjindaelmanaged Provider) to perform encryption. Two parameters are very important, the Key and IV(initial vector). I suggest you ask the fusion guy to directly give you the two things (better in byte array format/hex encoded) which can be directly passed into the AES provider's Key and IV property. Therefore, it's much more convenient for you to first test out whether the main AES provider settings are correct. After that, we can move onto the password derived approach.

BTW, in your code, you first use Unicode Encoding to convert string to byte, you need to also confirm with Fusion guys that whether they also use unicode encoding or only use base64 encoding for all string-bytes conversion. This is also very important.

Sincerely,

Steven Cheng

Microsoft MSDN Online Support Lead

Delighting our customers is our #1 priority. We welcome your comments and suggestions about how we

can improve the support we provide to you. Please feel free to let my manager know what you think of

the level of service provided. You can send feedback directly to my manager

at: msdnmg@xxxxxxxxxxxxxxxx

=====
Get notification to my posts through email? Please refer to

<http://msdn.microsoft.com/en-us/subscriptions/aa948868.aspx#notifications>.

Note: MSDN Managed Newsgroup support offering is for non-urgent issues where an initial response from

the community or a Microsoft Support Engineer within 2 business day is acceptable. Please note that

each follow up response may take approximately 2 business days as the support professional working

with you may need further investigation to reach the most efficient resolution. The offering is not

appropriate for situations that require urgent, real-time or phone-based

Re: Web app security

interactions. Issues of this

nature are best handled working with a dedicated Microsoft Support Engineer by contacting Microsoft

Customer Support Services (CSS) at <http://msdn.microsoft.com/en-us/subscriptions/aa948874.aspx>

=====
This posting is provided "AS IS" with no warranties, and confers no rights.

From: "SAL" <SAL@xxxxxxxxxxxxxx>
Subject: Web app security
Date: Mon, 27 Oct 2008 14:45:49 -0700

Hello,
at our company we have two different web development platforms, ASP.NET

and

ColdFusion.
We are trying to merge security between the platforms to provide a

security

blanket, so-to-speak, around all our apps.
We are trying to come up with the same encryption for a simple string with

a

simple Key using AES encryption. Since AES uses Rijndael I'm using that algorithm.

I admit my understanding of this is very limited but here's what we are trying. The ColdFusion guy says he has different encoding options when

using

AES, one being Base64 encoding.

We are trying to encrypt the following string and come up with the same results:

string = 'mystring'
password = 00000000000000000000000000000000

Re: Web app security

Salt = ALgzpd1HvwRonMPzOPDp7g==

I've read through the docs a few times and am still not making sense of this. I need to be able to match the ColdFusion guys output. He's outputting:

Using Base64 encoding:

sZ4SKYHMO6At4GJP1i+QFA==

The docs for his function are at:

<http://livedocs.adobe.com/coldfusion/8/htmldocs/help.html?content=functions>

_e-g_01.html

He is not passing in the iterations argument.

So, I am using the following code:

The first function calling the second one.

```
public static string Encrypt(string clearText, string Password)
```

```
{  
    // First we need to turn the input string into a byte array.  
    byte[] clearBytes = System.Text.Encoding.Unicode.GetBytes(clearText);  
    byte[] salt =  
    System.Text.Encoding.Unicode.GetBytes("ALgzpd1HvwRonMPzOPDp7g==");
```

```
    PasswordDeriveBytes pdb = new PasswordDeriveBytes(Password,  
    new byte[] { 0x49, 0x76, 0x61, 0x6e, 0x20, 0x4d, 0x65, 0x64,
```

0x76,

```
    0x65, 0x64, 0x65, 0x76 });
```

```
    byte[] b = { 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
```

0x0,

```
    0x0, 0x0,  
    0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,  
    0x0, 0x0, 0x0, 0x0,  
    0x0, 0x0, 0x0, 0x0, 0x0, 0x0 };
```

```
    // I've tried it both ways here using the salt for the second argument
```

for

the pdb passwordDerivedBytes constructor.

```
byte[] encryptedData = Encrypt(clearBytes, b, salt);
```

```
//byte[] encryptedData = Encrypt(clearBytes, pdb.GetBytes(32),  
pdb.GetBytes(16));
```

Re: Web app security

```
return Convert.ToBase64String(encryptedData);
}

public static byte[] Encrypt(byte[] clearData, byte[] Key, byte[] IV)
{
    // Create a MemoryStream that is going to accept the encrypted bytes
    MemoryStream ms = new MemoryStream();

    // Create a symmetric algorithm.
    // We are going to use Rijndael because it is strong and available on all
    // platforms.
    // You can use other algorithms, to do so substitute the next line with
    // something like
    // TripleDES alg = TripleDES.Create();

    Rijndael alg = Rijndael.Create();
    // I tried this next line to no avail
    //alg.Mode = CipherMode.ECB;

    alg.Key = Key;
    //alg.IV = IV;

    // Create a CryptoStream through which we are going to be pumping our
data.

    // CryptoStreamMode.Write means that we are going to be writing data to
the
stream
// and the output will be written in the MemoryStream we have provided.

    CryptoStream cs = new CryptoStream(ms, alg.CreateEncryptor(),
CryptoStreamMode.Write);

    // Write the data and make it do the encryption

    cs.Write(clearData, 0, clearData.Length);

    cs.Close();

    byte[] encryptedData = ms.ToArray();
    return encryptedData;
}
```

Re: Web app security